ABSTRACT

In order to create a highly-secured common key while a data error on a transmission path is corrected by an error correction code having remarkably high characteristics, in a quantum key distribution method of the invention, at first a communication apparatus on a reception side corrects the data error of reception data by a deterministic, stable-characteristics parity check matrix for a "Irregular-LDPC code." The communication apparatus on the reception side and a communication apparatus on a transmission side discard a part of pieces of the common information according to public error correction information.